CLAIMS

Having thus described my invention, what I claim as new and desire to secure by Letters Patent is as follows:

1. A verification method comprising verifying ownership of an electronic receipt in a communication system providing a public key encryption infrastructure, including the steps of:

   receiving a message from a sender, said message being electronically signed by said sender using a private signature key owned by said sender, said message includes a receipt which is electronically signed by an issuer having given said receipt using a private signature key assigned to said issuer, wherein said receipt includes details for what said receipt has been given and a reference to said owner of said receipt;

   obtaining a public signature verification key on the basis of said reference to said owner of said receipt; and

   examining whether or not said private signature key used for electronically signing said message is associated to said public signature verification key obtained on the basis of said reference to said owner of said receipt.

2. The method according to claim 1, wherein said reference to said owner of said receipt is a public signature verification key associated to a private signature key held by said owner of said receipt.

3. The method according to claim 1, wherein said reference to said owner of said receipt is a pseudonym used by said owner of the receipt.

4. The method according to claim 3, wherein obtaining said public signature verification key on the basis of said pseudonym used by said owner of said receipt includes getting a certificate securely linking said pseudonym to said public signature verification key.

5. The method according to claim 1, further comprising the step of authenticating said receipt using a public signature verification key assigned to said issuer of said receipt.

6. A receipt generation method, comprising generating an electronic receipt in a communication system providing a public key encryption system, including the steps of:

receiving a message from a sender, said message is electronically signed by said sender using a private signature key owned by said sender, whereby said message includes a transaction request and a reference to a designated owner of a receipt to be generated;

authenticating said message using a public signature verification key associated to said private signature key held by said sender of said message;

issuing a receipt including said reference to said designated owner of said receipt and details for what said receipt has been given; and

electronically signing said receipt with a public signature key assigned to an issuer issuing said receipt.

7. The method according to claim 6, further including the steps of performing said requested transaction, and returning said receipt to said sender.

8. The method according to claim 6, wherein said sender uses an anonymous communication connection.

9. The method according to claim 6, wherein said sender uses a pseudonym for communicating.

10. The method according to claim 6, wherein said reference to a designated owner is a pseudonym used by said designated owner.

11. The method according to claim 6, wherein said designated owner of the receipt is the sender.

12. The method according to claim 6, wherein said reference to a designated owner is a public signature key associated to a private signature verification key held by said designated owner of said receipt.

13. A method for proving ownership of a receipt, the method comprising proving ownership of said receipt in a communication system providing a public key encryption infrastructure, including the steps of:

creating a first message including a transaction request and a reference to a designated owner of a receipt to be generated in response to receiving said message;

electronically signing said message using a first private signature key;

sending said first message to a first addressee; and

receiving said receipt from said first addressee, said receipt being electronically signed by said first addressee having given said receipt using a private signature key assigned to said first addressee, wherein said receipt includes information as for what said receipt has been issued and said reference to said designated owner of said receipt.

14. The method according to claim 13, further comprising:

creating a second message including said receipt;

electronically signing said second message using a second private signature key; and

sending said second message to a second addressee;

15. The method according to claim 13, wherein the first addressee is identical to the second addressee.

16. The method according to claim 13, wherein the first private signature key is identical to the second private signature key.

17. The method according to claim 13, wherein said reference to said designated owner of said receipt is a pseudonym used by said owner of the receipt.

18. The method according to claim 13, wherein said reference to said designated owner of said receipt is a public signature verification key associated to a

private signature key held by said owner of said receipt.

19. The method according to claims 13, wherein said designated owner of said receipt is identical to a sender sending said first message to the first addressee.

20. The method according to claim 13, further comprising:

creating a second message including said receipt; electronically signing said second message using a second private signature key; and

sending said second message to said designated owner of said receipt.

21. The method according to claim 13, wherein said steps of sending and receiving of the first message and second message is performed over an anonymous communication connection.

22. The method according to claim 13, wherein said sending and receiving of the first message and second message is performed by using a pseudonym.

23. A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method according to claim 1.

24. A verification device comprising:

means for receiving a message from a sender, said message is electronically signed by said sender using a private signature key owned by said sender, said message includes a receipt which is electronically signed by an issuer having given said receipt using a private signature key assigned to said issuer, wherein said receipt includes details for what said receipt has been given and a reference to an owner of said receipt;

means for obtaining a public signature verification key on the basis of said reference to said owner of said receipt; and

means for examining whether or not said private signature key used for electronically signing said message is associated to said public signature verification key obtained on the basis of said reference to said owner of said receipt, said device being for verifying ownership of said receipt in a communication system providing a public key encryption infrastructure.

25. A receipt generating device comprising:

means for receiving a message from a sender, said message is electronically signed by said sender using a private signature key owned by said sender, whereby said message includes a transaction request and a reference to a designated owner of a receipt to be generated;

means for authenticating said message using a public signature verification key associated to said private signature key held by said sender of said message;

means for issuing a receipt including said reference to said designated owner of said receipt and details for what said receipt has been given; and

means for electronically signing said receipt with a public signature key assigned to an issuer issuing said receipt, said device being for generating said receipt in a communication system providing a public key encryption system.

26. A device for proving ownership of a receipt, said device comprising:

means for creating a first message including a transaction request and a reference to a designated owner of the receipt to be generated in response of receiving said message;

means for electronically signing said message using a first private signature key;

means for sending said first message to a first addressee;

means for receiving a receipt from said first addressee, which is electronically signed by said first addressee having given said receipt using a private signature key assigned to said first addressee, wherein said receipt includes information related to a purpose for which said receipt has been given, and related to said reference to said designated owner of said receipt,

said device being for proving ownership of the receipt in a communication system providing a public key encryption infrastructure.

27. A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method according to claim 6.

28. A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method according to claim 13.

29. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for [DESCRIPTION OF GENERAL FUNCTION], said method steps comprising:

30. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for verification, said method steps comprising the steps of claim 1.

31. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for receipt generation, said method steps comprising the steps of claim 6.

32. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for proving ownership of a receipt, said method steps comprising the steps of claim 13.

33. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing receipt verification, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of the device in claim 24.

34. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing receipt generation, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of the device in claim 25.

35. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing proof of receipt ownership, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of the device in claim 26.